Security+

Cybersecurity

Certification Prep Day 2

Class Objectives

By the end of class, you will be able to:

- Explain how each domain is divided across the Security+ exam.
- Prepare for Security+ questions from domains we have not explored in the curriculum, such as Architecture and Design and Identity and Access Management.
- Correctly answer Security+ practice questions.

The first half of today's class will focus on several domains on the exam and the types of questions they contain.

The second half of the class will be a fun quiz competition using a program called Kahoot.

Security+ Domains

Security+ Exam Topics Breakdown

Domain Distribution

01 Threats, Attacks, and Vulnerabilities

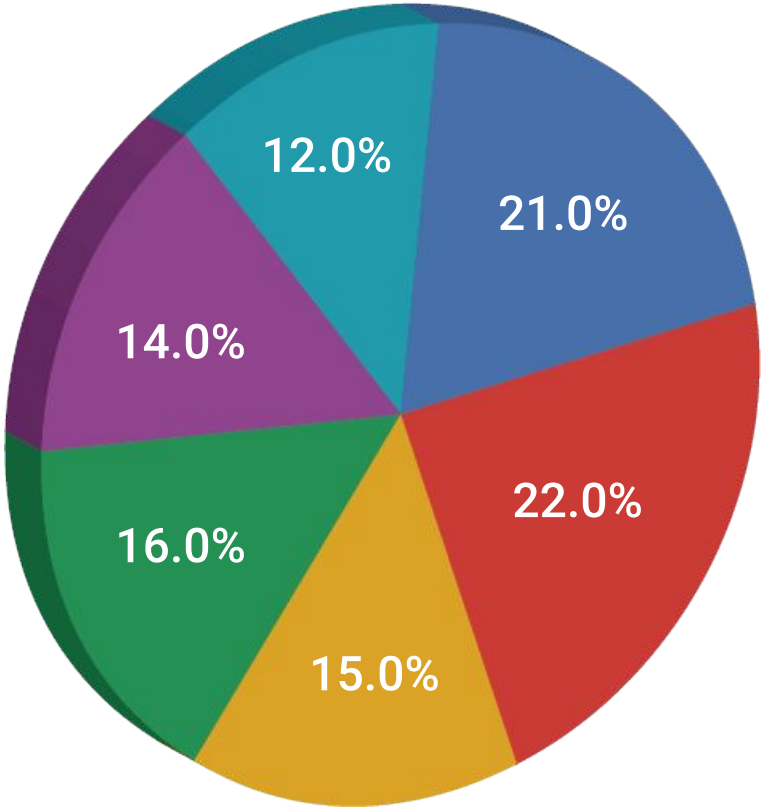
02 Technologies and Tools

03 Architecture and Design

04 Identity and Access Management

05 Risk Management

06 Cryptography and PKI



Security+ Exam Domains

Our course has covered many topics in these four domains:

Today, we'll take some time to look at the **Identity and Management** and **Architecture and Design** domains.

Identity & Access Management (IAM)

Identity and Access Management

Identity and Access Management covers the security policies that ensure an organization's resources are only accessible by the right people, for the right reasons, at the right times.

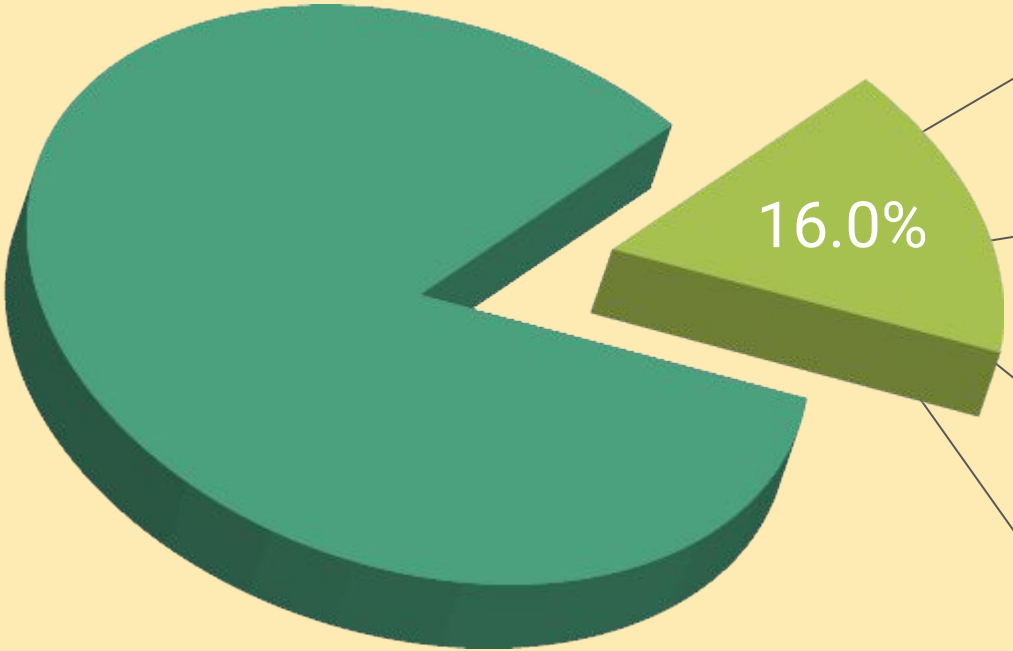
There are significant risks to incorrectly assigning access to resources.

Identity and Access Management

For example, if an organization gives all staff access to payroll databases, the staff would be able to view PII and other private data of the organization and its employees.

Identity and Access Management

The IAM domain makes up 16% of the exam's questions and covers the following subtopics:



01 Compare and contrast identity and access management concepts.

02 Given a scenario, install and configure identity and access services.

03 Given a scenario, implement identity and access management controls.

04 Given a scenario, differentiate common account management practices.

01

Compare and contrast identity and access management concepts.

This subdomain focuses on the basic terms and concepts associated with IAM, such as:

Authentication, Authorization, and Accounting (AAA): the framework to best control access to an organization's resources.

Types of authentication factors:

Something you are.
Includes biometrics, such as retina scanning or facial recognition.

Something you have.
Such as tokens or key-cards.

Something you know.
Such as PINs or passwords.

Example Question:

Of the following authentication factors, which one is a different factor than a retina scan?

A. Hand geometry recognition
B. Voice recognition
C. Fingerprint recognition
D. Proximity cards

Example Question:

Of the following authentication factors, which one is a different factor than a retina scan?

A. Hand geometry recognition
B. Voice recognition
C. Fingerprint recognition
D. **Proximity cards**

- Proximity cards are “something you have” while the other options are all biometric factors (“something you are”).

02

Given a scenario, install and configure identity and access services.

This subdomain focuses on the the application of the concepts associated with IAM, such as authentication protocols like **Kerberos**, **CHAP**, and **PAP**.

Kerberos	**Kerberos** is an authentication protocol developed at MIT that works using tickets.
PAP	**Password Authentication Protocol (PAP)** uses a standard username and password to authenticate to a remote system and is considered insecure.
CHAP	**Challenge-Handshake Authentication Protocol (CHAP)** uses a three-way handshake, making it more secure than PAP.

Example Question:

Which of the following authentication protocols is considered insecure due to its lack of encryption?

A. EAP
B. SAP
C. PAP
D. CHAP

Example Question:

Which of the following authentication protocols is considered insecure due to its lack of encryption?

A. EAP
B. SAP
C. **PAP**
D. CHAP

- PAP is insecure and unencrypted.

03

Given a scenario, implement identity and access management controls.

This subdomain focuses on management decisions for making sure the right people have access to the right resources for the right reasons.

Various types of access controls include:

- MAC — Mandatory Access Control (MAC)
- DAC — Discretionary Access Control (DAC)
- RBAC — Role Based Access Control (RBAC)

03

Given a scenario, implement identity and access management controls.

This topic also focuses on selecting the best access controls based on your organization's environment.

- For example, voice recognition is an appropriate biometric control if your office environment is relatively quiet.

Example Question:

For the following biometric controls, which would you select if you have a noisy office with good lighting and need a cost-efficient solution?

A. Voice recognition
B. DNA analysis
C. Fingerprint recognition
D. Speech recognition

Example Question:

For the following biometric controls, which would you select if you have a noisy office with good lighting and need a cost-efficient solution?

A. Voice recognition
B. DNA analysis
C. **Fingerprint recognition**
D. Speech recognition

- A and D would not be optimal in a noisy office, and B would likely be an expensive biometric solution.

04

Given a scenario, differentiate common account management practices.

This subdomain focuses on how user accounts are managed.

It includes the concept of least privilege, which students should be familiar with.

Account types:

User Accounts	The basic, standard account type for users at your organization. These accounts usually have limited privileges.
Guest Accounts	For non-employees who need limited access to your organization's resources.
Privileged Accounts	Greater access than user accounts and are provided to managers and system administrators.

Example Question:

An external auditor needs limited access to your organization. What type of account should you provide them?

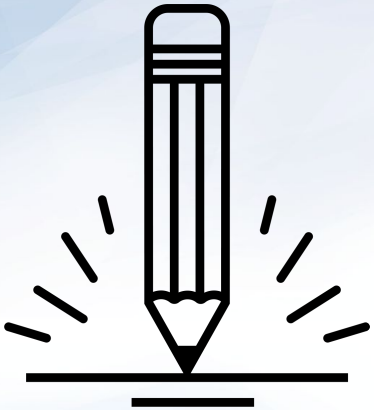
A. Guest account
B. User account
C. Sudo account
D. Service account

Example Question:

An external auditor needs limited access to your organization. What type of account should you provide them?

A. **Guest account**
B. User account
C. Sudo account
D. Service account

- You would provide a guest account to a non-employee who needs limited access.



Activity: Security+ IAM

In this activity, you will complete a quiz of PBQ and multiple choice questions from the Identity and Access Management domain.

Suggested Time:

Time’s Up! Let’s Review.

Security+ Architecture and Design Domain

Architecture and Design covers the processes and controls used to protect the confidentiality, integrity, and availability of an organization's data.

Architecture and Design

This domain consists of nine sub domains:

01	Explain use cases and purpose for frameworks, best practices, and secure configuration guides.
02	Given a scenario, implement secure network architecture concepts.
03	Given a scenario, implement secure systems design.
04	Explain the importance of secure staging deployment concepts.
05	Explain the security implications of embedded systems.
06	Summarize secure application development and deployment concepts.
07	Summarize cloud and virtualization concepts.
08	Explain how resiliency and automation strategies reduce risk.
08	Explain the importance of physical security controls.

Architecture and Design

We'll focus on the following four:

01	Explain use cases and purpose for frameworks, best practices, and secure configuration guides.
02	Given a scenario, implement secure network architecture concepts.
03	Given a scenario, implement secure systems design.
04	Explain the importance of secure staging deployment concepts.
05	Explain the security implications of embedded systems.
06	Summarize secure application development and deployment concepts.
07	Summarize cloud and virtualization concepts.
08	Explain how resiliency and automation strategies reduce risk.
09	Explain the importance of physical security controls.

05

Explain the security implications of embedded systems.

This subdomain focuses on the security of **embedded systems**, which are systems that have hardware with software embedded within them.

For example, a **smart refrigerator** is an example of an embedded system.

A smart refrigerator has hardware and software embedded within it to complete specific tasks, such as:

- Monitoring temperature.
- Determining if a filter needs replacing.

Architecture and Design

Terms to know include:

01 **Supervisory Control and Data Acquisition (SCADA)**

SCADA is a system used to control technical equipment in industries such as:

- Energy
- Oil
- Water management

02 **Internet of Things (IoT)**

IoT is the network of devices that are connected to the internet, which is considered an extension of the internet itself.

- Smart light bulbs
- Smart refrigerators
- Printers
- Door locks

IoT is an expansive term relevant to many areas such as smart houses, research and monitoring in the healthcare industry, wearable devices such as step counters, data collection in agriculture, manufacturing and city management and many, many more.

Example Question:

To protect their data, which type of systems are usually not connected to the internet?

A. Linux servers
B. Apache web servers
C. SCADA systems
D. Home office networks

Example Question:

To protect their data, which type of systems are usually not connected to the internet?

A. Linux servers
B. Apache web servers
C. **SCADA systems**
D. Home office networks

- While some SCADA systems have limited connection to the internet, they run high impact systems so are usually are not connected.

06

Summarize secure application development and deployment concepts.

This subdomain focuses on the concepts and processes relevant to developing secure applications for organizations and their users.

- For instance, **input validation** restricts what data can be input to application fields, such as limiting non-ASCII characters.

Software development methodologies:

Agile

Agile is a flexible development method that allows changes to the development requirements.

Waterfall

Waterfall is a structured and rigid development method where each step of development cycle depends on the previous step.

Example Question:

What is the biggest risk of outputting detailed application errors with coding details?

A. There is no risk, and it is recommended.

B. Coding details could provide the developer's name.

C. Coding details could illustrate vulnerabilities in the application code, which a hacker can then exploit.

D. Coding details could show when the code was written.

Example Question:

What is the biggest risk of outputting detailed application errors with coding details?

A. There is no risk, and it is recommended.

B. Coding details could provide the developer's name.

C. **Coding details could illustrate vulnerabilities in the application code, which a hacker can then exploit.**

D. Coding details could show when the code was written.

- Displaying the code details, such as the coding language, version and structure, could provide vulnerability information to hackers to exploit.

08

Explain how resiliency and automation strategies reduce risk.

This subdomain focuses on the processes associated with maintaining a business's services when there are disruptions.

High Availability	Describes a system that is available for a long period of time, typically as close to 100% as possible.
Scalability	The ability for your organization's technology to easily grow and manage increased demand.
Snapshot	The state of a virtual machine at a certain point in time.

Example Question:

Which of the following is the process of constantly checking systems for attacks, threats, vulnerabilities, and other risks?

A. Continuous monitoring
B. Redundancy
C. Fault tolerance
D. RAID

Example Question:

Which of the following is the process of constantly checking systems for attacks, threats, vulnerabilities, and other risks?

A. Continuous monitoring
B. Redundancy
C. Fault tolerance
D. RAID

- Continuous monitoring is the process constantly checking systems for attacks, threats, vulnerabilities, and other risks.

09

Explain the importance of physical security controls.

This subdomain focuses on concepts associated with physical security processes and controls.

Environmental Controls

Such as HVAC systems and fire suppression systems.

Physical Access Controls

Such as gates, man traps, and security guards.
Physical control types include:

- **Deterrents** such as alarms.
- **Preventions** such as locks or gates

Example Question:

What type of risk can a bollard protect against?

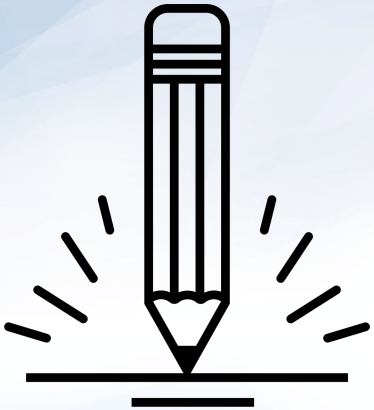
A. Fire
B. Flooding
C. Vehicle Access
D. Script Kiddies

Example Question:

What type of risk can a bollard protect against?

A. Fire
B. Flooding
C. **Vehicle access**
D. Script kiddies

- A bollard is a short post that's built into the ground to protect areas from vehicle access.



Activity: Security+ Architecture and Design

In this activity, you will take a quiz made of PBQ and multiple choice questions from the Architecture and Design domain.

Suggested Time:

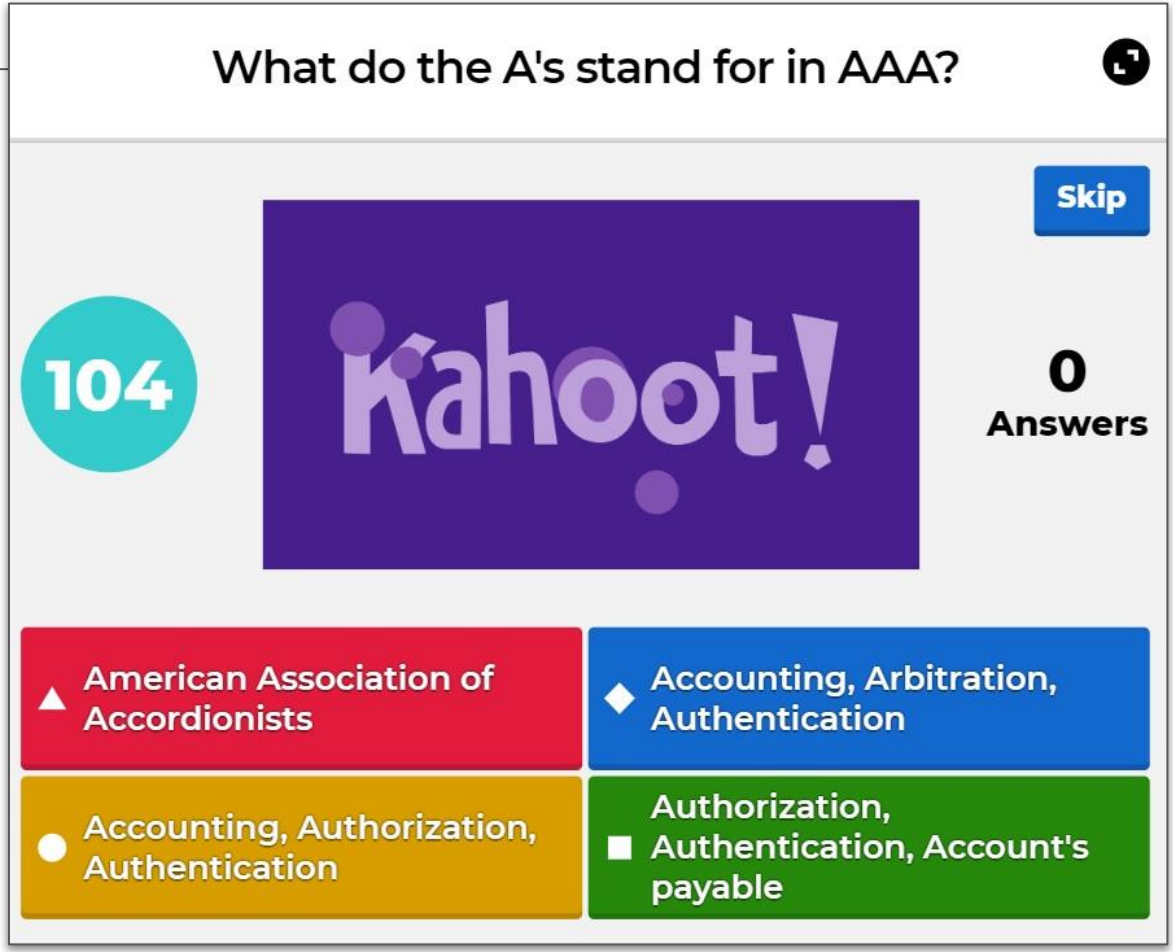
Time’s Up! Let’s Review.

Now, we will take part in a fun and challenging competition using:

What's Kahoot?

Kahoot is a web-based tool that:

- Displays questions and answers for students to select from in real-time.
- Keeps track of individual and team scores.
- Keeps track of remaining time for each question.



(kahoot.com)

Kahoot! Rules and Guidelines

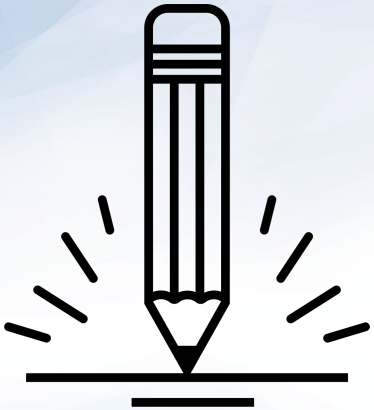
- There are a total of 30 Security+ questions.
- Points are not deducted for incorrect answers.
- You will have two minutes to answer each question.
- If you are competing as a team, select a team captain to answer the questions.
- Points are awarded for correct answers and for how quickly you answer the questions compared to your classmates.
- **Note:** If your class is currently online, it will be easier if each student competes individually.

(kahoot.com)

Kahoot! Rules and Guidelines

- The questions will come from any of the six Security+ domains.
- You can use all available resources: books, the internet, class notes, etc.
- Any issues will be decided by the judges (the TAs and/or instructor), e.g.:
  - Answer disputes
  - Frozen or lagging computers
  - Kahoot issues
- The team or individual with the most points at the end of 30 questions is the winner!

(kahoot.com)



Activity: Kahoot Challenge

Now we'll begin the competition!

Suggested Time:


The End.